13

by A L

Submission date: 11-Jun-2021 04:08PM (UTC+0700)
Submission ID: 1604613200
File name: 24006-61917-1-PB.pdf (941.83K)
Word count: 5967
Character count: 20628

Scientific Journal of Informatics
Vol. 7, No. 1, May 2020
p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

A Novel Construction of Perfect Strict Avalanche Criterion S-box using Simple Irreducible Polynomials

Alamsyah

Department of Computer Science, Universitas Negeri Semarang Sekaran Campus, Gunungpati, Semarang, 50229, Indonesia
Email: alamsyah@mail.unnes.ac.id

Abstract

An irreducible polynomial is one of the main components in building an S-box with an algebraic technique approach. The selection of the precise irreducible polynomial will determine the quality of the S-box produced. One method for determining good S-box quality is strict avalanche criterion will be perfect if it has a value of 0.5. Unfortunately, in previous studies, the strict avalanche criterion value of the S-box produced still did not reach perfect value. In this paper, we will discuss S-box construction using selected irreducible polynomials. This selection is based on the number of elements of the least amount of irreducible polynomials that make it easier to construct S-box construction. There are 17 irreducible polynomials that meet these criteria. The strict avalanche criterion test results show that the irreducible polynomial $p_{17}(x) = x^8 + x^7 + x^6 + x + 1$ is the best with a perfect SAC value of 0.5. One indicator that a robust S-box is an ideal strict avalanche criterion value of 0.5

Keywords: Strict Avalanche Criterion, S-box, Irreducible Polynomial, Algebraic Technique

1. INTRODUCTION

S-box which is also known as a substitution box has a function in the process of randomizing data bits [1]. The strength of the S-box generated will determine the durability of a message that has been encrypted from linear and differential attacks [2]. The method used in constructing S-box construction in this paper is algebraic techniques. In algebraic techniques, irreducible polynomials play an important role in making S-box construction [3]. An irreducible polynomial is a polynomial that has two multiplication factors, namely itself and 1 [4]. In GF ((2^8)), the irreducible polynomial that is built has the highest degree of 8 which is used to make a multiplicative inverse. The resulting multiplicative inverse will be used to build an S-box. Hence, the role of the irreducible polynomial is crucial in building a strong S-box construction [5].

One of the criteria for determining the strength of an S-box is the perfect value of the strict avalanche criterion (SAC) [1]. The SAC is used to see changes that occur in input bits and output bits. If there is a change in 1-bit of input, ideally there should be half of the output bit changed. This means that the perfect SAC value is 0.5 [6]. The SAC value produced by the S-boxes construction that has been carried out by previous researchers is various. Girija and Singh [7] developed S-boxes with a double random phase encoding (DRPE) system. Farwa et al. [8] built an S-box with a specific nonlinear and iterative map approach. Çavuşoğlu et al. [9] developed an S-box design by placing an 8-bit value taken from a random number generator (RNG).

Hussain et al. [10] built S-box construction based on quantum magnets and Lorenz chaotic system matrix. Belazi et al. [11], Özkaynak et al. [12], Özkaynak and Yavuz [13], Liu et al. [14], Khan et al. [15], and Khan and Syah [16] proposed S-boxes based on a chaotic system. Proposed S-boxes were also developed by [17], [18], [19], [20], [21], [22], and [23]. Unfortunately, the resulting SAC value [7-23] is only close to the perfect value of 0.5.

In this paper, we will present S-boxes construction using simple irreducible polynomials. S-boxes are built based on 17 simple irreducible polynomials, i.e., $p_1(x)$, $p_2(x)$, …, $p_{17}(x)$. The resulting S-boxes will be tested using SAC. The proposed S-box is the selected S-box that has the best SAC value compared to previous studies. In the next section, we will discuss the irreducible polynomial.

2. METHODS

2.1. Irreducible Polynomial

An irreducible polynomial is a polynomial that has two multiplication factors, i.e., itself and 1. Table 1 shows the irreducible polynomials classified according to the order of the number of the smallest polynomial elements [24] as listed in [25], [26], [27], [28], and [29]. Based on Table 1, 17 irreducible polynomials have the least number of polynomial elements, namely five elements. Through 17 selected irreducible polynomials, the multiplicative inverse will be built.

Table 1. Number Of Irreducible Polynomials Elements

Irreducible Polynomials	Number of elements
$x^8+x^4+x^3+x+1$	5
$x^8+x^4+x^3+x^2+1$	5
$x^8+x^5+x^3+x+1$	5
$x^8+x^5+x^3+x^2+1$	5
$x^8+x^5+x^4+x^3+1$	5
$x^8+x^6+x^3+x^2+1$	5
$x^8+x^6+x^5+x+1$	5
$x^8+x^6+x^5+x^2+1$	5
$x^8+x^6+x^5+x^3+1$	5
$x^8+x^6+x^5+x^4+1$	5
$x^8+x^7+x^2+x+1$	5
$x^8+x^7+x^3+x+1$	5
$x^8+x^7+x^3+x^2+1$	5
$x^8+x^7+x^5+x+1$	5
$x^8+x^7+x^5+x^3+1$	5
$x^8+x^7+x^5+x^4+1$	5
$x^8+x^7+x^6+x+1$	5
$x^8+x^5+x^4+x^3+x^2+x+1$	7
$x^8+x^6+x^4+x^3+x^2+x+1$	7
$x^8+x^6+x^5+x^4+x^2+x+1$	7
$x^8+x^6+x^5+x^4+x^3+x+1$	7
$x^8+x^7+x^4+x^3+x^2+x+1$	7

$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$	7
$x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$	7
$x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$	7
$x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1$	7
$x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$	7
$x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$	7
$x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$	7
$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$	7

Further discussion of multiplicative inverse construction is presented in the novel S-boxes construction section.

2.2. Novel S-Boxes Construction

In this section, we will introduce S-box construction based on simple irreducible polynomial specifically irreducible polynomial which has the least polynomial elements. The S-box construction proposed based on the scheme in Figure 1. According to Figure 1, the S-box construction is generated from a multiplicative inverse applied to affine mapping. The affine mapping consists of an affine matrix and the addition of a constant 8-bit vector as shown in Eq. (1).

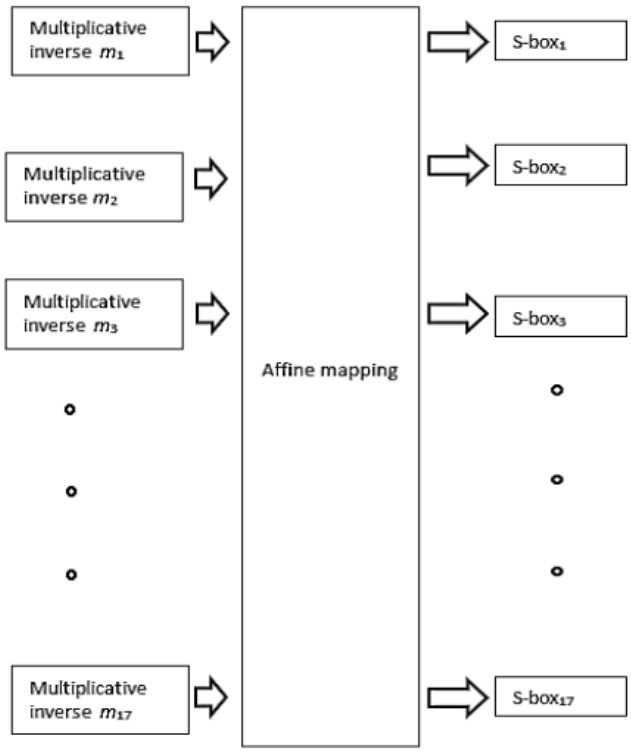

Figure 1. The construction scheme for the proposed S-boxes

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,1\,1 \\ 1\,1\,0\,0\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0\,0\,1\,1 \\ 1\,1\,1\,1\,0\,0\,0\,1 \\ 1\,1\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,0\,0 \\ 0\,0\,1\,1\,1\,1\,1\,0 \\ 0\,0\,0\,1\,1\,1\,1\,1 \end{bmatrix} \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \qquad (1)$$

For example, S-box$_1$, S-box$_2$, and S-box$_3$ will be built using irreducible polynomials $p_1(x) = x^8 + x^4 + x^3 + x + 1$, $p_2(x) = x^8 + x^4 + x^3 + x^2 + 1$, and $p_3(x) = x^8 + x^5 + x^3 + x + 1$. Tables 2, 3 and 4 are multiplicative inverse tables of m_1, m_2, and m_3, respectively, which are built based on the irreducible polynomials. Each inverse multiplicative is applied to Eq. (1) so that Tables 5, 6 and 7 are obtained which are S-box$_1$, S-box$_2$, and S-box$_3$, respectively.

Table 2. The proposed multiplicative inverse m_1

0	1	141	246	203	82	123	209	232	79	41	192	176	225	229	199
116	180	170	75	153	43	96	95	88	63	253	204	255	64	238	178
58	110	90	241	85	77	168	201	193	10	152	21	48	68	162	194
44	69	146	108	243	57	102	66	242	53	32	111	119	187	89	25
29	254	55	103	45	49	245	105	167	100	171	19	84	37	233	9
237	92	5	202	76	36	135	191	24	62	34	240	81	236	97	23
22	94	175	211	73	166	54	67	244	71	145	223	51	147	33	59
121	183	151	133	16	181	186	60	182	112	208	6	161	250	129	130
131	126	127	128	150	115	190	86	155	158	149	217	247	2	185	164
222	106	50	109	216	138	132	114	42	20	159	136	249	220	137	154
251	124	46	195	143	184	101	72	38	200	18	74	206	231	210	98
12	224	31	239	17	117	120	113	165	142	118	61	189	188	134	87
11	40	47	163	218	212	228	15	169	39	83	4	27	252	172	230
122	7	174	99	197	219	226	234	148	139	196	213	157	248	144	107
177	13	214	235	198	14	207	173	8	78	215	227	93	80	30	179
91	35	56	52	104	70	3	140	221	156	125	160	205	26	65	28

Table 3. The proposed multiplicative inverse m_2

0	1	142	244	71	167	122	186	173	157	221	152	61	170	93	150
216	114	192	88	224	62	76	102	144	222	85	128	160	131	75	42
108	237	57	81	96	86	44	138	112	208	31	74	38	139	51	110
72	137	111	46	164	195	64	94	80	34	207	169	171	12	21	225
54	95	248	213	146	78	166	4	48	136	43	30	22	103	69	147
56	35	104	140	129	26	37	97	19	193	203	99	151	14	55	65
36	87	202	91	185	196	23	77	82	141	239	179	32	236	47	50
40	209	17	217	233	251	218	121	219	119	6	187	132	205	254	252
27	84	161	29	124	204	228	176	73	49	39	45	83	105	2	245
24	223	68	79	155	188	15	92	11	220	189	148	172	9	199	162
28	130	159	198	52	194	70	5	206	59	13	60	156	8	190	183
135	229	238	107	235	242	191	175	197	100	7	123	149	154	174	182
18	89	165	53	101	184	163	158	210	247	98	90	133	125	168	58
41	113	200	246	249	67	215	214	16	115	118	120	153	10	25	145
20	63	230	240	134	177	226	241	250	116	243	180	109	33	178	106
227	231	181	234	3	143	211	201	66	212	232	117	127	255	126	253

Table 4. The proposed multiplicative inverse m_3

0	1	149	230	223	187	115	164	250	133	200	85	172	206	82
125	39	215	248	100	89	191	163	86	80	103	154	41	51	161
171	145	134	232	254	225	124	17	50	28	185	48	202	118	196
43	184	40	29	166	177	77	63	129	97	140	90	197	47	76
192	244	221	68	67	220	116	252	127	143	229	198	62	54	157
25	87	14	104	201	11	24	81	101	21	59	141	98	151	139
128	57	92	150	20	88	155	26	83	15	205	217	179	158	138
213	242	165	6	70	253	45	203	247	226	130	237	38	16	142
96	56	122	236	251	9	34	233	180	194	110	94	58	91	126
170	33	210	183	231	2	99	93	31	160	27	102	219	78	109
153	30	190	23	7	114	52	176	241	239	144	32	12	207	189
167	53	159	108	136	195	211	147	49	42	222	5	208	174	162
64	245	137	181	46	60	75	228	10	84	44	119	216	106	13
188	175	146	182	243	112	249	18	204	107	79	156	69	66	186
255	37	121	246	199	74	3	148	35	135	235	234	131	123	240
238	168	113	212	65	193	227	120	19	214	8	132	71	117	36

In the same way, it can be constructed S-box$_4$, S-box$_5$, S-box$_6$, S-box$_7$, S-box$_8$, S-box$_9$ S-box$_{10}$, S-box$_{11}$, S-box$_{12}$, S-box$_{13}$, S-box$_{14}$, S-box$_{15}$ S-box$_{16}$, and S-box$_{17}$. Each S-box produced will be tested using SAC. SAC is defined in the following Eq. (2) [3]:

$$S(x) = \left(\frac{1}{2^n}\sum_{i=1}^{n} f(x) \oplus f(x \oplus c_i^n)\right) \quad (2)$$

where n is the number of variables, and i is a 1-bit value in position ith. In detail, the process of calculating SAC value in S-box$_1$ is illustrated in Tables 8, 9, and 10.

Table 5. The proposed S-box$_1$

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187

Table 6. The proposed S-box$_2$

99	124	86	69	249	82	112	56	148	134	65	229	234	201	206
34	136	43	173	200	203	32	5	29	96	54	236	15	205	125
195	83	150	74	71	23	4	42	182	218	55	98	194	53	80
92	11	226	58	115	10	164	239	85	190	142	232	214	231	241
51	240	193	185	35	30	77	31	113	20	89	40	208	26	199
137	161	191	104	243	84	227	88	179	52	242	102	64	217	44
252	8	237	140	25	87	207	63	107	119	109	223	128	76	37
120	197	141	61	47	224	28	81	3	235	33	39	144	176	131
75	41	16	9	50	175	180	254	67	110	221	27	116	160	93
106	127	216	1	196	122	198	209	186	94	101	97	139	132	118
22	210	184	105	13	21	230	0	145	168	248	245	153	155	68
177	171	114	158	17	7	91	170	72	59	62	111	126	219	181
172	178	108	18	36	6	46	167	228	100	121	147	143	45	247
103	169	211	123	222	133	135	152	146	151	244	78	250	165	117
238	212	138	57	174	225	246	38	255	202	24	130	220	159	192
233	149	157	14	66	73	251	204	154	166	48	213	19	156	12

Table 7. The proposed S-box$_3$

99	124	126	138	127	39	151	115	255	143	211	54	139	145
45	221	135	193	59	178	91	46	23	85	26	219	103	80
214	2	174	48	131	215	50	141	79	22	25	113	237	244
89	6	120	9	77	225	63	212	243	88	104	147	72	37
43	69	65	216	133	94	202	189	19	73	171	105	203	51
117	8	217	191	204	186	106	74	36	241	168	119	121	64
236	150	209	95	238	173	196	84	116	198	176	61	223	167
185	7	108	33	230	162	27	242	100	246	210	83	194	146
71	137	112	76	224	132	190	47	130	21	253	239	183	140
201	159	228	163	149	93	102	206	55	15	75	5	3	30
250	40	68	207	62	136	13	254	38	109	29	128	231	142
82	18	184	195	20	10	251	60	110	70	96	0	218	181
164	90	11	157	58	245	125	180	165	41	4	235	34	129
122	170	35	188	24	182	222	172	175	158	1	153	199	154

156	227	81	123	118	98	66	97	161	177	17	14	205	111
114	247	169	166	187	52	233	78	179	152	155	144	249	213

Table 8. Bit input S-box$_1$

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	1
0	0	0	0	0	1	0	0
0	0	0	0	0	1	0	1
0	0	0	0	0	1	1	0
0	0	0	0	0	1	1	1
0	0	0	0	1	0	0	0
0	0	0	0	1	0	0	1
0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	1
0	0	0	0	1	1	0	0
0	0	0	0	1	1	0	1
0	0	0	0	1	1	1	0
0	0	0	0	1	1	1	1
0	0	0	1	0	0	0	0
0	0	0	1	0	0	0	1
0	0	0	1	0	0	1	0
0	0	0	1	0	0	1	1
0	0	0	1	0	1	0	0
0	0	0	1	0	1	0	1
0	0	0	1	0	1	1	0
0	0	0	1	0	1	1	1
0	0	0	1	1	0	0	0
0	0	0	1	1	0	0	1
0	0	0	1	1	0	1	0
0	0	0	1	1	0	1	1
0	0	0	1	1	1	0	0
0	0	0	1	1	1	0	1
0	0	0	1	1	1	1	0
0	0	0	1	1	1	1	1
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
1	1	1	1	1	0	0	0
1	1	1	1	1	0	0	1
1	1	1	1	1	0	1	0
1	1	1	1	1	0	1	1
1	1	1	1	1	1	0	0
1	1	1	1	1	1	0	1
1	1	1	1	1	1	1	0
1	1	1	1	1	1	1	1

Table 9. Bit output S-box$_1$

0	1	1	0	0	0	1	1
0	1	1	1	1	1	0	0
0	1	1	1	0	1	1	1
0	1	1	1	1	0	1	1
1	1	1	1	0	0	1	0
0	1	1	0	1	0	1	1
0	1	1	0	1	1	1	1
1	1	0	0	0	1	0	1
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	1
0	1	1	0	0	1	1	1
0	0	1	0	1	0	1	1
1	1	1	1	1	1	1	0
1	1	0	1	0	1	1	1
1	0	1	0	1	0	1	1
0	1	1	1	0	1	1	0
1	1	0	0	1	0	1	0
1	0	0	0	0	0	1	0
1	1	0	0	1	0	0	1
0	1	1	1	1	1	0	1
1	1	1	1	1	0	1	0
0	1	0	1	1	0	0	1
0	1	0	0	0	1	1	1
1	1	1	1	0	0	0	0
1	0	1	0	1	1	0	1
1	1	0	1	0	1	0	0
1	0	1	0	0	0	1	0
1	0	1	0	1	1	1	1
1	0	0	1	1	1	0	0
1	0	1	0	0	1	0	0
0	1	1	1	0	0	1	0
1	1	0	0	0	0	0	0
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
0	1	0	0	0	0	0	1
1	0	0	1	1	0	0	1
0	0	1	0	1	1	0	1
0	0	0	0	1	1	1	1
1	0	1	1	0	0	0	0
0	1	0	1	0	1	0	0
1	0	1	1	1	0	1	1
0	0	0	1	0	1	1	0

Table 10. Values of the first row SAC matrix S-box$_1$

0	0	0	1	1	1	1	1
0	0	0	1	1	1	1	1
0	0	0	0	1	1	0	0
0	0	0	0	1	1	0	0
1	0	0	1	1	0	0	1
1	0	0	1	1	0	0	1
1	0	1	0	1	0	1	0
1	0	1	0	1	0	1	0
0	0	1	1	0	0	0	1
0	0	1	1	0	0	0	1
0	1	0	0	1	1	0	0
0	1	0	0	1	1	0	0
0	0	1	0	1	0	0	1
0	0	1	0	1	0	0	1
1	1	0	1	1	1	0	1
1	1	0	1	1	1	0	1
0	1	0	0	1	0	0	0
0	1	0	0	1	0	0	0
1	0	1	1	0	1	0	0
1	0	1	1	0	1	0	0
1	0	1	0	0	0	1	1
1	0	1	0	0	0	1	1
1	0	1	1	0	1	1	1
1	0	1	1	0	1	1	1
0	1	1	1	1	0	0	1
0	1	1	1	1	0	0	1
0	0	0	0	1	1	0	1
0	0	0	0	1	1	0	1
0	0	1	1	1	0	0	0
0	0	1	1	1	0	0	0
1	0	1	1	0	0	1	0
1	0	1	1	0	0	1	0
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
1	1	0	1	1	0	0	0
1	1	0	1	1	0	0	0
0	0	1	0	0	0	1	0
0	0	1	0	0	0	1	0
1	1	1	0	0	1	0	0
1	1	1	0	0	1	0	0
1	0	1	0	1	1	0	1
1	0	1	0	1	1	0	1
128	116	124	116	144	116	132	132

3. RESULT AND DISCUSSION

The number of variables in GF(2^8) is 8. The values of $\sum_{i=1}^{n} f(x) \oplus f(x \oplus c_i^n)$ are 128, 116, 124, 116, 144, 116, 132, and 132. According to Eq. (2), the values of the SAC matrix produced by the first row are 0.5, 0.453125, 0.484375, 0.453125, 0.5625, 0.453125, 0.515625, and 0.515625. The complete SAC S-box$_1$ matrix is shown in Table 11. Based on Table 11, the average SAC value in S-box$_1$ is 0.50488. The average values of SAC in other proposed S-boxes, i.e, S-box$_2$, S-box$_3$, S-box$_4$, ..., S-box$_{17}$ are shown in Table 12.

Table 11. The SAC matrix of the proposed S-box$_1$

0.5	0.453125	0.484375	0.45313	0.5625	0.453125	0.515625	0.515625
0.5313	0.5	0.453125	0.48438	0.5	0.5625	0.484375	0.46875
0.5	0.53125	0.5	0.5625	0.46875	0.5	0.515625	0.515625
0.5469	0.5	0.53125	0.5	0.453125	0.46875	0.53125	0.53125
0.5313	0.546875	0.5	0.5	0.515625	0.453125	0.5	0.453125
0.5313	0.53125	0.546875	0.46875	0.46875	0.515625	0.515625	0.453125
0.4844	0.53125	0.53125	0.46875	0.515625	0.46875	0.53125	0.53125
0.5156	0.484375	0.53125	0.48438	0.53125	0.515625	0.5625	0.515625

Table 12. The SAC mean values of the proposed S-box$_1$ to S-box$_{17}$

S-boxes	SAC
Proposed S-box$_1$	0.50488
Proposed S-box$_2$	0.49658
Proposed S-box$_3$	0.50635
Proposed S-box$_4$	0.51343
Proposed S-box$_5$	0.50806
Proposed S-box$_6$	0.49585
Proposed S-box$_7$	0.49951
Proposed S-box$_8$	0.50757
Proposed S-box$_9$	0.51025
Proposed S-box$_{10}$	0.50073
Proposed S-box$_{11}$	0.49780
Proposed S-box$_{12}$	0.49780
Proposed S-box$_{13}$	0.50781
Proposed S-box$_{14}$	0.50220
Proposed S-box$_{15}$	0.49292
Proposed S-box$_{16}$	0.50757
Proposed S-box$_{17}$	**0.50000**

According to Table 12, the perfect SAC value is found in the proposed S-box$_{17}$ with a value of 0.5. Thus, the best S-box is the proposed S-box$_{17}$. The multiplicative inverse table m_{17} and proposed S-box$_{17}$ are shown in Tables 13 and 14. Table 15 shows the

values of the SAC matrix from the proposed S-box$_{17}$. In the next section, we will discuss the SAC performance analysis of each S-box produced in previous studies that will be compared with the best S-box, i.e., proposed S-box$_{17}$.

Table 13. The proposed multiplicative inverse m_{17}

0	1	225	190	145	106	95	129	169	127	53	101	206	83	161	38
181	163	222	30	251	118	211	49	103	208	200	148	177	35	19	223
187	244	176	29	111	108	15	160	156	93	59	241	136	205	249	195
210	23	104	97	100	10	74	218	185	174	240	42	232	132	142	147
188	113	122	139	88	246	239	124	214	221	54	219	230	167	80	170
78	171	207	13	252	158	153	114	68	247	135	165	157	41	128	6
105	51	234	237	52	11	209	24	50	96	5	144	37	110	109	36
189	65	87	152	120	196	21	250	116	197	66	138	71	238	168	9
94	7	217	242	61	233	164	90	44	204	123	67	150	199	62	146
107	4	143	63	27	201	140	198	115	86	178	183	40	92	85	253
39	14	180	17	134	91	231	77	126	8	79	81	173	172	57	184
34	28	154	182	162	16	179	155	175	56	245	32	64	112	3	224
213	226	248	47	117	121	151	141	26	149	228	255	137	45	12	82
25	102	48	22	227	192	72	220	243	130	55	75	215	73	18	31
191	2	193	212	202	254	76	166	60	133	98	236	235	99	125	70
58	43	131	216	33	186	69	89	194	46	119	20	84	159	229	203

Table 14. The proposed S-box$_{17}$

99	124	215	68	2	129	240	243	232	19	18	36	145	116	16	194
157	46	96	40	224	244	251	110	26	218	211	97	225	161	179	127
39	69	254	9	226	195	198	15	153	206	168	38	20	176	222	10
228	207	191	88	59	165	98	28	25	181	57	70	48	144	86	60
122	169	112	53	173	123	109	50	152	65	51	3	138	82	85	201
30	214	142	248	189	167	250	136	216	100	177	108	134	103	236	33
160	80	14	83	13	186	197	106	79	71	0	29	227	253	220	252
101	187	8	229	78	87	241	255	202	72	154	42	249	114	247	132
239	62	61	7	234	47	115	147	4	175	111	133	95	118	203	35
158	31	73	212	75	204	104	105	151	23	192	163	120	209	54	162
221	217	130	141	174	140	149	63	12	155	1	74	148	139	150	6
190	22	219	188	49	146	223	196	170	137	90	128	164	182	66	200
185	246	193	37	213	81	64	119	84	126	180	156	11	27	231	107
117	5	113	208	233	43	92	94	24	210	44	125	135	67	172	55
91	93	52	166	237	131	32	77	245	143	121	76	17	102	45	230
183	89	205	34	159	56	199	178	21	58	235	238	41	184	171	242

Table 15. The SAC matrix of the proposed S-box$_{17}$

0.5469	0.4531	0.4531	0.4531	0.4688	0.4531	0.5313	0.5
0.5	0.5469	0.5	0.5156	0.5469	0.4688	0.5469	0.4375
0.4375	0.5	0.4844	0.5	0.5156	0.5469	0.5156	0.4844
0.4844	0.4375	0.5	0.4688	0.4844	0.5156	0.5156	0.5469
0.5469	0.4844	0.5313	0.5156	0.4688	0.4844	0.4688	0.5
0.5	0.5469	0.5469	0.4844	0.5156	0.4688	0.5156	0.5313
0.5313	0.5	0.5313	0.5156	0.4688	0.5156	0.5469	0.5313
0.5313	0.5313	0.4688	0.5	0.4688	0.4688	0.4375	0.4844

3.1. Performance Analysis of The Novel S-Boxes

Table 16 shows the performance comparison of SAC values from S-boxes that were previously made. Based on Table 16, the proposed S-box$_{17}$ has the best SAC value of 0.5.

Table 16. Performance comparison

S-boxes	SAC
AES	0.5048
In [7]	0.5107
In [8]	0.5066
In [9]	0.5064
In [10]	-
In [11]	0.4956
In [12]	0.4983
In [13]	0.5036
In [14]	0.4976
In [15]	0.4930
In [16]	0.4978
In [17]	0.503
In [18]	0.503
In [19]	0.504
In [20]	0.502
In [21]	0.498
In [22]	0.5002
In [23]	0.5017
Proposed S-box$_{17}$	**0.5000**

According to the previous discussion about S-box construction, it can be concluded that the proposed S-box$_{17}$ has a perfect SAC value and is the best value compared to the S-box results of previous studies.

4. CONCLUSION

In this research, a novel method was introduced in building S-box construction to get the perfect SAC value. The S-box construction starts with classifying the irreducible polynomial based on the number of the least polynomial elements (simple irreducible polynomial). The selection of simply reduced polynomials aims to simplify calculations in building multiplicative inverse. The results of each element of the multiplication inverse are applied to the affine matrix and the addition of a constant 8-bit vector to produce an S-box. This result shows that the proposed S-box17 has a perfect SAC value of 0.5. So it can be concluded that the proposed S-box has the best SAC value compared to the S-boxes from the previous research. For the next research, it is expected that there will be further research in S-box construction that has perfect value other than the SAC criteria in a good S-box test.

5. REFERENCES

[1] Wu, C. K., & Feng, D. (2016). *Boolean functions and their applications in cryptography*. Springer Berlin Heidelberg.

[2] Hussain, I., & Shah, T. (2013). Literature survey on nonlinear components and chaotic nonlinear components of block ciphers. *Nonlinear Dynamics*, *74*(4), 869-904.

[3] Daemen, J., & Rijmen, V. (2002). *The design of Rijndael (Vol. 2)*. New York: Springer-verlag.

[4] C. Paar and J. Pelzl. (2010). *Understanding Cryptography*, 1st ed., vol. 1. Springer-Verlag Berlin Heidelberg.

[5] Alamsyah, Bejo, A., & Adji, T. B. (2017, August). AES S-box construction using different irreducible polynomial and constant 8-bit vector. In *2017 IEEE Conference on Dependable and Secure Computing (pp. 366-369)*. IEEE.

[6] Williams, H., Webster, A., & Tavares, S. (1986). On the design of s-boxes. In *Advances in Cryptology—CRYPTO'85 Proceedings* (Vol. 218, pp. 523-534).

[7] Girija, R., & Singh, H. (2018). Enhancing security of double random phase encoding based on random S-Box. *3D Research*, *9*(2), 15.

[8] Farwa, S., Muhammad, N., Shah, T., & Ahmad, S. (2017). A novel image encryption based on algebraic S-box and Arnold transform. *3D Research, 8*(3), 26.

[9] Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos, Solitons & Fractals, 95,* 92-101.

[10] Hussain, I., Anees, A., AlKhaldi, A. H., Algarni, A., & Aslam, M. (2018). Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications. *Chinese Journal of Physics, 56*(4), 1609-1621.

[11] Belazi, A., Khan, M., El-Latif, A. A. A., & Belghith, S. (2017). Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. *Nonlinear Dynamics, 87*(1), 337-361.

[12] Özkaynak, F., Çelik, V., & Özer, A. B. (2017). A new S-box construction method based on the fractional-order chaotic Chen system. *Signal, Image and Video Processing*, *11*(4), 659-664.

[13] Özkaynak, F., & Yavuz, S. (2013). Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dynamics, 74*(3), 551-557.

[14] Liu, G., Yang, W., Liu, W., & Dai, Y. (2015). Designing S-boxes based on 3-D four-wing autonomous chaotic system. *Nonlinear Dynamics, 82*(4), 1867-1877.
[15] Khan, M., Shah, T., Mahmood, H., Gondal, M. A., & Hussain, I. (2012). A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dynamics, 70*(3), 2303-2311.
[16] Khan, M., & Shah, T. (2015). An efficient construction of substitution box with the fractional chaotic system. *Signal, Image, and Video Processing, 9*(6), 1335-1338.
[17] Lambić, D. (2017). A novel method of S-box design based on a discrete chaotic map. *Nonlinear Dynamics, 87*(4), 2407-2413.
[18] Khan, M., & Azam, N. A. (2015). S-boxes based on affine mapping and orbit of power function. *3D Research, 6*(2), 12.
[19] Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., & Kaçar, S. (2017). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dynamics, 87*(2), 1081-1094.
[20] Ullah, A., Jamal, S. S., & Shah, T. (2017). A novel construction of substitution box using a combination of chaotic maps with improved chaotic range. *Nonlinear Dynamics, 88*(4), 2757-2769.
[21] Isa, H., Jamil, N., & Z'aba, M. R. (2016). Construction of cryptographically strong S-Boxes inspired by bee waggle dance. *New generation computing, 34*(3), 221-238.
[22] Ul Islam, F., & Liu, G. (2017). Designing S-box based on 4D-4wing hyperchaotic system. *3D Research, 8*(1), 9.
[23] Hussain, I., Gondal, M. A., & Hussain, A. (2015). Construction of Substitution Box Based on Piecewise Linear Chaotic Map and S 8 Group. *3D Research, 6*(1), 3.
[24] Stallings, W. (2014). *Cryptography and network security: principles and practice, international edition: principles and practice*. Pearson Higher Ed.
[25] Gangadari, B. R., & Ahamed, S. R. (2015, August). Analysis and algebraic construction of S-Box for AES algorithm using irreducible polynomials. In *2015 Eighth International Conference on Contemporary Computing (IC3)* (pp. 526-530). IEEE.
[26] Wang, D., & Sun, S. L. (2008, December). Replacement and Structure of S-boxes in Rijndael. In *2008 International Conference on Computer Science and Software Engineering* (Vol. 3, pp. 782-784). IEEE.
[27] Alamsyah, Bejo, A., & Adji, T. B. (2018). The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box. *Nonlinear Dynamics, 93*(4), 2105-2118.
[28] Alamsyah, Bejo, A., & Adji, T. B. (2018, October). S-box Construction of Highly Strict Avalanche Criterion Using Algebraic Technique. In *2018 Third International Conference on Informatics and Computing (ICIC)* (pp. 1-4). IEEE.
[29] Alamsyah, Bejo, A., & Adji, T. B. (2019, October). Enhancement strict avalanche criterion value in robust S-boxes construction using selected irreducible polynomial and affine matrixes. In *Journal of Physics: Conference Series* (Vol. 1321, No. 3, p. 032020). IOP Publishing.

ORIGINALITY REPORT

14%	7%	12%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Zhongyun Hua, Jiaxin Li, Yongyong Chen, Shuang Yi. "Design and application of an S-box using complete Latin square", Nonlinear Dynamics, 2021 Publication	2%
2	www.cs.wvu.edu Internet Source	2%
3	docplayer.info Internet Source	2%
4	Hilman Wisnu, Muhammad Afif, Yova Ruldevyani. "Sentiment analysis on customer satisfaction of digital payment in Indonesia: A comparative study using KNN and Naïve Bayes", Journal of Physics: Conference Series, 2020 Publication	1%
5	Alamsyah, Agus Bejo, Teguh Bharata Adji. "The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box", Nonlinear Dynamics, 2018 Publication	1%
6	es.scribd.com Internet Source	1%

7	Alamsyah. "Improving the Quality of AES S-box by Modifications Irreducible Polynomial and Affine Matrix", 2020 Fifth International Conference on Informatics and Computing (ICIC), 2020 Publication	1 %
8	Alamsyah, Agus Bejo, Teguh Bharata Adji. "AES S-box construction using different irreducible polynomial and constant 8-bit vector", 2017 IEEE Conference on Dependable and Secure Computing, 2017 Publication	1 %
9	Yuanyuan Zhou, François-Xavier Standaert. "Deep learning mitigates but does not annihilate the need of aligned traces and a generalized ResNet model for side-channel attacks", Journal of Cryptographic Engineering, 2019 Publication	<1 %
10	link.springer.com Internet Source	<1 %
11	Maitra, S.. "Results on multiples of primitive polynomials and their products over GF(2)", Theoretical Computer Science, 20050905 Publication	<1 %
12	Sadam Hussain, Sajjad Shaukat Jamal, Tariq Shah, Iqtadar Hussain. "A Power Associative Loop Structure For The Construction Of	<1 %

Non-Linear Components Of Block Cipher", IEEE Access, 2020
Publication

---

13 Zhiliang Zhu, Yanjie Song, Wei Zhang, Hai Yu, Yuli Zhao. "A novel compressive sensing-based framework for image compression-encryption with S-box", Multimedia Tools and Applications, 2020 <1 %
Publication

---

14 A. Lempel. "Analysis and synthesis of polynomials and sequences over<tex>GF(2) </tex>", IEEE Transactions on Information Theory, 1971 <1 %
Publication

---

15 Atta Ullah, Sajjad Shaukat Jamal, Tariq Shah. "A novel scheme for image encryption using substitution box and chaotic system", Nonlinear Dynamics, 2017 <1 %
Publication

---

16 Lecture Notes in Computer Science, 2015. <1 %
Publication

---

17 Mohamed Saber, Esam Hagras. "Parallel multi-layer selector S-Box based on lorenz chaotic system with FPGA implementation", Indonesian Journal of Electrical Engineering and Computer Science, 2020 <1 %
Publication

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13